REMARKS

The present Amendment amends claims 9, 10, 12, 21, 22, 24, 33, 34 and 36, leaves claims 11, 23 and 35 unchanged and adds new claim 38. Therefore, the present application has pending claims 9-12, 21-24 and 33-36 and 38.

Claims 9-12 stand rejected under 35 USC §101 being that the Examiner alleges that the claimed invention is directed to non-statutory subject matter particularly a computer program. With respect to the rejection of claims 9-12, it should be noted that claims 9-12 are now directed to a method performed by a computer. Therefore, this rejection is overcome and should be withdrawn.

Claims 9-12, 21-24 and 33-36 stand rejected under 35 USC §112, first paragraph as allegedly being based on a disclosure which is not enabling and claims 9-12, 21-24 and 33-36 stand rejected under 35 USC §112, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. These rejections with respect to claims 9-12, 21-24 and 33-36 are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 9-12, 21-24 and 33-36 fully comply with the requirements of 35 USC §112, and as such the subject matter recited in the claims are in fact based on a disclosure that is enabling and the subject matter as recited in the claims is complete being that the essential elements of the invention are recited in the claims. Therefore, reconsideration and withdraw of these rejections is respectfully requested.

It should be noted that the claims as amended are based on a disclosure that is enabling being that the claims now recite a dividing plaintext operation or step which corresponds to the flowchart and the corresponding description of Fig. 2, a generating first and second random number blocks operation or step which corresponds to the flowchart and corresponding description of Fig. 3 and performing decryption operations and concatenating the series of ciphertext blocks operations or steps which correspond to the flowcharts and corresponding description of Fig. 5. Therefore, the claims as now written are in fact based on an enabling disclosure.

In the Office Action the Examiner alleges that essential elements are omitted from the claims and identifies such essential elements as two computers connected over a network, padding, a pseudo-random sequence, a counter, a series of ciphertext blocks, and concatenates the series of ciphertext blocks one after another sequentially. Applicants submit that the elements identified by the Examiner are not essential elements of the invention and as such need not be recited in the claims. However, the claims were amended to recite that the method is performed by a computer, that first and second random number blocks are generated, that a series of ciphertext blocks are produced and that such series of ciphertext blocks are concatenated.

Therefore, based on the above, Applicants respectfully request the Examiner to reconsider and withdraw the 35 USC §112, first and second paragraphs rejections.

Claims 9-12, 21-24 and 33-36 stand rejected under 35 USC §102(e) as being anticipated by Shukla (U.S. Patent No. 6,345,101); and claims 11, 12, 23, 24, 35 and

36 stand rejected under 35 USC §103(a) as being unpatentable over Shukla in view of Davis. These rejections are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 9-12, 21-24 and 33-36 are not taught or suggested by Shukla or Davis whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw these rejections.

Amendments were made to the claims so as to more clearly describe features of the present invention. Particularly, amendments were made to the claims in order to more clearly describe that the present invention is directed to a symmetric key encryption method, apparatus, computer program and program product as recited, for example, in independent claims 9, 21 and 33. The present invention as recited in said claims provides:

(1) a first random number block and a second random number block are applied to the same plaintext block i throughout the decryption operation related to the plaintext block i, and

(2) an intermediate result of decryption operation performed on the plaintext block i-i is used, as a feedback value, for another decryption operation performed on the plaintext block i that follows.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record particularly Shukla or Davis whether taken individually or in combination with each other as suggested by the Examiner.

Shukla discloses a cryptographic method that belongs to a symmetric-key decryption method and generates a random number block corresponding to a ciphertext block. However, there is no teaching or suggestion in Shukla of the decryption operation of the present invention as recited in the claims.

Shukla's decryption operation consists of a series of rounds. Each of the ciphertext blocks goes through one series of the rounds. One of the rounds consists of an X0R3 operation, a shuffle operation and an XOR1 operation, and these operations are executed in this order, as shown at column 3, lines 22-37. The XOR3 operation performs an XOR operation among the bit strings of a ciphertext block E. The shuffle operation shuffles the bits of the result (E1) of the XOR3 operation in accordance with each bit value of the complement K' of a private key K. The XORT operation performs an XOR operation on the result (E2) of the shuffle operation and a random number block S.

The decryption operation as recited in the claims includes first, second and third operations which are quite different from the teachings of Shukla. For example, the third operation step in the present invention as recited in the claims uses the second random number block, whereas Shukla's third operation (the XOR1 operation) does not use a random number block as in the present invention.

Further, for example, the first operation step in the present invention as recited in the claims as performed on the ciphertext block i uses, as a feedback value, a result of the second operation step that has been performed on the ciphertext block i-1, whereas Shukla's round operations on a ciphertext block E do

not use a result of the operations performed on another ciphertext block as in the present invention.

Thus, Shukla fails to teach or suggest performing decryption operations for producing plaintext blocks each corresponding to each of the plurality of ciphertext blocks and concatenating the series of the ciphertext blocks one after another sequentially to output a plaintext which includes a message and redundancy data series as recited in the claims.

Further, Shukla fails to teach or suggest that one of the decryption operations for producing the plaintext block i corresponding to the ciphertext i ($2 \leq i \leq$ a number of plaintext blocks) comprises a first operation step for performing an arithmetic computation on the ciphertext block i, a second operation step for performing an arithmetic operation on a result of the first operation step performed on the ciphertext block i and the first random number block corresponding to the ciphertext block i, and a third step for performing an arithmetic computation on a result of the second operation step performed on the ciphertext block i and a second random number block corresponding to the ciphertext block i-1, to produce the plaintext block i as recited in the claims.

Still further, Shukla fails to teach or suggest that the first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and that either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step as recited in the claims.

Therefore, Shukla fails to teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §102(e) rejection of claims 9-12, 21-24 and 33-36 is respectfully requested.

The above described features of the present invention shown above not to be taught or suggested by Shukla are also are not taught or suggested by Davis. Thus, combining the teachings of Shukla and Davis in the manner suggested by the Examiner in the Office Action still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

Davis discloses an integrity check value (ICV) that accompanies a message. The ICV is used to determine whether the contents of a message have been modified during transmission.

Thus, it is quite clear that Davis does not teach or suggest numerous features of the present invention particularly those features shown above not to be taught or suggested by Shukla.

Therefore, the combination of Shukla and Davis still fails to teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 11, 12, 23, 24, 35 and 36 as being unpatentable over Shukla in view of Davis is respectfully requested.

The present Amendment adds new claim 38. New claim 38 depends from claim 22. Therefore, the same arguments presented above with respect to claim 22 apply as well to new claim 38. In addition, new claim 38 recites other features

particularly with regard to the random number generation circuit including a pseudo-random number generator and a circuit for producing the random number blocks. Such features are clearly not taught or suggested by any of the references of record, particularly Shukla and Davis, whether taken individually or in combination with each other.

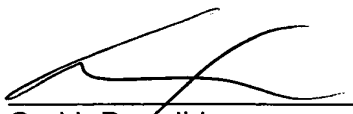
The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 9-12, 21-24 and 33-36.

In view of the foregoing amendments and remarks, applicants submit that claims 9-12, 21-24 and 33-36 and 38 are in condition for allowance. Accordingly, early allowance of claims 9-12, 21-24 and 33-36 and 38 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.39632VX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120